REMARKS/ARGUMENTS

Claims 1-48 are pending. Claims 1-25 have been withdrawn from consideration. Claims 26-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawe (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

The Examiner states that the sections in Hagerman and Hawe cited by the Applicants in the previous Office Action Response are not an accurate characterization of the Hagerman and Hawe references. It is respectfully submitted that the sections in Hagerman and Hawe were not intended to fully characterize the Hagerman and Hawe references but were merely included to provide some context for the discussion of the Hagerman and Hawe materials. It is acknowledged that it is not possible to provide a complete and accurate characterization of the Hagerman and Hawe references in their entirety simply by quoting single specific paragraphs.

The Examiner indicated that not all independent claims recite "receiving a frame at a first network entity from the second network entity" and "identifying a security control indicator in the frame from the second network entity." It is acknowledged that not all independent claims include this exact language. It is respectfully submitted that some of the claims are directed at a transmitter and others at a receiver. Consequently, all claims recite a second frame having a security control indicator. In some instances, the second frame is transmitted while in other instances the second frame is received. However, it is respectfully submitted that all independent claims include recitations not taught or suggested by the references cited by the Examiner either alone or in combination. For example, the independent claims all variably recite a first fibre channel frame including a security enable indicator wherein the first fibre channel frame is associated with a fabric login or a port login message. The independent claims also all variably recite a security control indicator in a second fibre channel frame, wherein the security control indicator is used to determine if the frame is encrypted and authenticated. In some instances, the frames are transmitted. In other instances, the frames are received. The materials cited by the Examiner either alone or in combination do not teach or suggest these recitations.

The Examiner relies on Hawes to describe these recitations. The Examiner appears to cite column 8 lines 6-23 and column 10, lines 45-60 on page 6 of the Office Action.

"In accordance with one of the protocols described in this specification, encryption is performed at a transmitting or source node and decryption is performed at a destination node. This is known as end-to-end encryption, as contrasted with link encryption, in which decryption and re-encryption are performed at each intermediate node between the source and the destination. The manner in which encryption is performed, or the encryption algorithm, is of no particular consequence to the present invention. Nor is it of any consequence whether encryption and decryption keys are exchanged in advance between the sending and receiving nodes, or whether a public key system is used for the establishment of keys. As will be noted later in this description, one implementation of the invention uses an encryption algorithm known as the Data Encryption Standard (DES), as defined by FIPS-46 (Federal Information Processing Standard-46) published by the National Institute of Standards and Technology (formerly the National Bureau of Standards). However, the invention is not limited to this, or any other encryption algorithm." (Hawes: column 8, lines 6-23)

"The identification of every conceivable packet format would be complex and time-consuming. Moreover, the present invention is not limited to parsing logic capable of identifying particular packet formats. By way of example, several types of formats are identified in the receive data path of a presently preferred embodiment of the invention. These formats are shown diagrammatically in FIGS. 9a-9b, 10 and 11. FIGS. 9a-9b show two variants of the packet format known as SNAP/SAP, including a Data Link encryption format defined by Digital Equipment Corporation (FIG. 9a), and the DOD-IP encryption format (FIG. 9b). FIG. 10 shows the ISO end-to-end encryption packet format, and FIG. 11 shows a third format, known as SILS, which is still in the process of being defined in the industry." (Hawes: column 10, lines 45-60)

The material cited by the Examiner does not teach or suggest any security enable indicator. The material cited describes various encryption formats, but does not teach or suggest any first frame having a security enable indicator and a second frame having a security control indicator. It is theoretically possible that a security enable indicator is included in a first frame, but this is not taught of suggested in the materials cited by the Examiner and can not be assumed.

Furthermore, it is respectfully submitted that none of the materials teach or suggest including any security enable indicator in the first frame where the first frame is associated with a fabric login or port login message. It is acknowledged that theoretically security enable indicators can be used, but none of the references cited teach or suggest including these

indicators in fabric login or port login messages. Hawes does not use any fabric login or port login messages because Hawes describes a packet network system that does not have any fabric login or port login mechanisms. Hagerman similarly is not believed to teach or suggest using any login, fabric login, port login, flogi, or plogi messages to include a security enable indicator.

According to various embodiments, "The techniques of the present invention include security in initialization messages such as PLOGI, FLOGI, and other classes of messages such as SW_ILS, FC-CT, ELS and ELP. According to various embodiments, the techniques of the present invention embed a security enable parameter in an authentication message. When a new network entity is introduced into a fibre channel fabric, the new network entity transmits an initialization message with the security enable parameter. The receiving network entity may or may not support security. If the receiving network entity supports authentication, the receiving network entity can extract the security enable parameter and transmit a response acknowledging authentication capabilities. Other information can be exchanged during an authentication sequence to provide for future security in transmissions between the two network entities. In one example, the two entities can exchange cryptographic material in the authentication sequence to allow common key generation." (page 11, lines 19-31)

Furthermore, "Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security." (page 20, lines 3-7)

CONCLUSION

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Audrey Kwan/

G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100